REMARKS

Reconsideration and allowance of the above-referenced application are respectfully requested. Claims 2, 14, 23, 31, 38, 50, 59, and 71 are canceled. Claims 1, 3, 5, 7-8, 10-12, 15-22, 27, 30, 37, 44, 47, 58, 65, and 68 have been amended. Claims 1, 3-13, 15-22, 24-30, 32-37, 39-49, 51-58, 60-70, and 72-78 are pending in the application.

Review of Claim Language

Each of the claims have been amended to specify that any encryption or decryption is distinct from the requesting device.

For example, independent claims 1, 22, 37, and 58 as amended specify that the unified communications system receives the message ***in unencrypted form from the requesting device*** as part of the user interface session, and that the resource (invoked for executing encryption) and the executing encryption are ***distinct from the requesting device***. Hence, claims 1, 22, 37, and 58 as amended explicitly distinguish from encryption that is performed by the requesting device.

Independent claims 11, 30, 47, and 68 as amended specify that the resource invoked for attempting decrypting is ***distinct from the requesting device*** that is requesting retrieval of the one stored message determined to be encrypted. Hence, claims 11, 30, 47, and 68 as amended explicitly distinguish from decryption that is performed by the requesting device.

The claims as amended also specify that the subscriber profile directory is distinct from the requesting device.

Hence, the claims as amended specify a unified communication system (or unified communications server) that receives a key *from* a requesting device, as part of a user interface session, in order to cause at least one of encryption or decryption of a message by a resource ***distinct from the requesting device***.

In addition, the independent claims explicitly specify that encryption/attempted decryption by the invoked resource is based on the encryption key/decryption key that ***is input by the user*** via the requesting device ***as part of the user interface session***.

Hence, each of the independent claims enable a user of the requesting device to send and/or receive encrypted messages, *regardless of whether any encryption / decryption utility is installed on the requesting device* that is in use by the user, based on **prompting** the user for an encryption/decryption key ***as part of the user interface session***, and **receiving** the encryption/decryption key ***as part of the user interface session***.

These and other features are neither disclosed nor suggested in the applied prior art.

Claims 1, 22, 37, and 58

A. U.S. Patent No. 6,442,600 to Anderson

1) No Generating *and Outputting to* the Requesting Device a First Prompt to Select Encryption

Applicant traverses the Official Action as incomplete because it fails to answer the material traversed. (See MPEP §707.07(f) "Where the applicant traverses any rejection, the examiner should, if he or she repeats the rejection, take note of the applicant's argument and answer the substance of it.").

The Examiner failed to respond to Applicant's Argument that Anderson does not teach a unified communications system / server / device executing a medium that generates ***for the requesting device*** as part of the user interface session a first prompt enabling the user to select encryption of the message. As admitted in the Official Action, Anderson fails to teach that the user interface session between the system / server and the ***requesting device*** is provided by the server. Hence, the assertion that Anderson discloses "generating for the requesting device as part of the user interface session a first prompt enabling the user to select encryption of the message" is without foundation.

Further, the claims as amended specify that the unified communications system / server / device executing a medium generates and outputs to the requesting device the prompts for the user to select encryption, and input the encryption key.

In fact, Anderson consistently teaches that all operations are performed *in the requesting device* by the message sender 154. Specifically, col. 5, lines 24-30 describes that **each recipient**

computer system 150 includes a Message Sender 154 and can store the server system's public key 157. Fig. 3 illustrates operations by the message sender routine, including determining in step 315 "whether the user has indicated to encrypt the message" (col. 8, lines 43-44); if encryption is selected, the Message Sender retrieves the locally stored server's public key, and the Message Sender *in the requesting device* encrypts the message in step 320 with the locally-retrieved server's key. The Message Sender then sends the message to the server in step 330 (see col. 5, lines 12-20 and 25-30; col. 8, lines 42-47).

Hence, Anderson neither discloses nor suggests that the unified communications system / server / device executing the medium generates ***and outputs to the requesting device*** a first prompt.

In fact, Anderson never generates a first prompt enabling the user to select encryption, but rather **detects** whether the user has **already** selected encryption (see, e.g., col. 5, lines 25-26 "[t]he ***sender can also indicate*** whether the message should be transmitted in an encrypted manner"; col. 8, lines 43-44 "[i]n step 315 it is determined whether the user has indicated to encrypt the message."): this is not a teaching of generating a first prompt (let alone by a server), but simply a detection of whether the user has selected encryption. Regardless, these operations are performed in the **requesting device**, and not in the server, as claimed.

2) No Invoking a Resource for Executing Encryption, by the System / Server, the Resource and the Executing Encryption being Distinct from the Requesting Device

The Examiner admits on page 4 that Anderson does not teach "a second prompt for the user to supply an encryption key", or "encrypting the message based on the encryption key received from the requesting device." Hence, the assertion by the Examiner that Anderson teaches "invoking a resource configured for executing encryption of the message into an encrypted message based on the encryption key" is inconsistent with the Examiner's admission that Anderson does not teach "encrypting the message based on the encryption key received from the requesting device."

Moreover, the claims as amended specify that the resource executing the encryption is ***distinct from the requesting device***. Hence, the claims as amended precludes any interpretation that would rely on the requesting device to perform the encryption, as disclosed in Anderson.

B. U.S. Patent No. 6,304,898 to Shiigi

Although discloses a "session" between Java Virtual Machines executed on the client computer 210 (Java VM 212) and the server computer 220 (Java VM 226) in Fig. 1B, there is no disclosure or suggestion of any encryption operations performed by the server.

Further, with respect to dependent claims 10, 29, 46, and 67 the HTTP server resource 221 in the server computer 220 is **distinct** from the Java VM 226; hence, there is no disclosure or suggestion in the hypothetical combination that the requests and responses could be received and sent according to HTTP and HTML protocol, since the Java connections are based on TCP/IP and remote method invocation methods (col. 6, lines 22-26); in fact, if Java was not used, then no "session" would be present (see, e.g., col. 10, lines 13-15).

C. U.S. Patent No. 5,870,477 to Sasaki

Applicant traverses the Official Action as incomplete because it fails to answer the material traversed. (See MPEP §707.07(f) "Where the applicant traverses any rejection, the examiner should, if he or she repeats the rejection, take note of the applicant's argument and answer the substance of it.").

The Examiner fails to address Applicant's traversal of the Examiner's assertion that Sasaki teaches "symmetric encryption of a message where a user inputs an encryption key for encrypting a centrally stored data/message. and where a select number of receivers are able to decrypt the data/message" (citations omitted).

As argued previously, this assertion is unsubstantiated, as **Sasaki provides no reference whatsoever to the term "symmetric encryption"**.

Further, the assertion does not resolve the Examiner's admissions on page 3 that Anderson does not teach "a second prompt for the user to supply an encryption key", or "encrypting the message based on the encryption key received from the requesting device." Rather, the Examiner's assertion simply addresses "the user to supply an encryption key" and "encrypting the message based on the encryption key", while disregarding the explicit claim limitation that ***encryption*** is based on the ***encryption*** key is ***received from the requesting device***.

Therefore, the rejection is legally deficient because it fails to address the claimed feature of the system/ server / device generating and outputting the second prompt ***to the requesting device***, or that the encryption is performed based on the encryption key ***received from the requesting device***.

Moreover, Sasaki also teaches that all encryption is performed in the client device (e.g., computer system 1 of Fig. 1, sending station 74 of Fig. 31). Column 41, line 46 to col. 42, line 20 explicitly require that the client device perform all encryption. As noted by the Examiner, Sasaki teaches with respect to Fig. 31 that a management key MA is sent by the sending station 74 to the receiving stations 75 and 77, but not the mail server 70 (col. 41, line 65 to col. 42, line 20). Hence, Sasaki teaches that it is impossible for the mail server 70 to either encrypt or decrypt any message!

Hence, Sasaki teaches away from the claimed feature of generating and outputting to the requesting device a second prompt for the user to input an encryption key, where the encryption is ***distinct from the requesting device***.

D. The Hypothetical Combination of Anderson, Shiigi, Sasaki, and Gifford

Hence, neither Sasaki, Shiggi, or Anderson, singly or in combination, disclose or suggest that the unified communications system / server / device executing the medium invokes the resource for executing encryption based on the encryption key ***received from the requesting device***, where the resource and executing encryption is ***distinct from the requesting device***, as claimed.

In fact, both Anderson and Sasaki consistently require that the ***client device*** perform the encryption. Given that Gifford is silent on how to perform any encryption, the hypothetical combination of Anderson, Shiigi, Sasaki, and Gifford still would require the encryption to be performed in the client device sending the message to the server.

For these and other reasons, the Examiner has failed to establish a prima facie case of obviousness; hence, the rejection of independent claims 1, 22, 37, and 58 should be withdrawn.

Claims 11, 30, 47, and 68

A. Anderson

1) No Subscriber Profile Directory

Applicant traverses the Official Action as incomplete because it fails to answer the material traversed. (See MPEP §707.07(f) "Where the applicant traverses any rejection, the examiner should, if he or she repeats the rejection, take note of the applicant's argument and answer the substance of it.").

The Examiner has failed to address Applicant's traversal of the Examiner's assertion that Anderson teaches "accessing, for the user interface session, subscriber profile information ***from a subscriber profile directory***": the Examiner's citation of "column 6, lines 5-67" fails to identify any reference whatsoever to the claimed subscriber profile directory. In fact, the cited portion provides no reference whatsoever to any data structure that can be considered a "subscriber profile directory".

Further, the claims as amended that the subscriber profile directory is distinct from the requesting device, hence, the client devices cannot be considered a teaching of the claimed subscriber profile directory.

In fact, Anderson provides no reference whatsoever to any of the claimed terms "subscriber", "profile", or "directory"!

B. Shiigi

Shiigi provides no disclosure or suggestion of any attempted decryption, let alone performing decryption by the resource distinct from the requesting device, as claimed.

C. Sasaki

The Examiner asserts that Sasaki teaches "symmetric encryption of a message where a user inputs an **encryption key for encrypting a centrally stored data / message**, and where a select number of **receivers are able to decrypt** the data/message by inputting a decryption key and **performing decryption of the message**." (Citations omitted)

As apparent from the foregoing, the rejection must be withdrawn because it fails to demonstrate that the hypothetical combination teaches the claimed "generating ***and outputting to the requesting device*** as part of the user interface session a prompt ... for the messaging subscriber to input a decryption key", and the claimed **system / server / device executing the medium** "invoking a resource configured for attempting decrypting ... based on the decryption key having been supplied ***by the messaging subscriber via the requesting device***", as claimed, where "the resource and the attempting decrypting being ***distinct from the requesting device***."

Rather, Sasaki teaches with respect to Fig. 31 (col. 41, line 45 to col. 42, line 20) that the receiving devices 75 and 77 receive the management key MA **from the sending station 74** (col. 41, lines 62-67); the receiving devices 75 and 77 read the enciphered file 1 (and including enciphered mail A and enciphered key KA) generated by the sending station 74 from the mail center 70, and the receiving devices 75 and 77 perform decryption **using the supplied management key MA from the sending station 74** (col. 42, lines 13-20).

Hence, Sasaki provides no disclosure or suggestion whatsoever of the claimed "generating a prompt ... for the messaging subscriber to ***input a decryption key***", because Sasaki explicitly teaches that the decryption key is **received from the sending station 74**.

In fact, Sasaki teaches that the decryption is performed exclusively in the receiving devices: it is impossible for the mail center 70 to invoke a resource for attempted decryption because the management key MA is never sent to the mail center 70.

Hence, the hypothetical combination does not disclose or suggest that the **unified communications system / server / device executing the medium** invokes a resource, ***distinct from the requesting device***, for attempted decryption based on generating a prompt for the

requesting device for the messaging subscriber to input a decryption key, the decryption key having been supplied by the messaging subscriber ***via the requesting device***.

For these and other reasons, the §103 rejection of the independent claims 11, 30, 47, and 68 should be withdrawn.

Dependent Claims

As noted previously, the Java-based connection between the server and the client teaches away from the claimed transfer information "as part of the user interface session" according to HTTP protocol, as specified for example in claims 10, 29, 46, and 67. For these and other reasons, the §103 rejection of these claims should be withdrawn.

The Examiner acknowledged during a telephonic interview on October 12, 2006 that the rejections of the dependent claims should have included the Shiigi reference. It is believed the remaining dependent claims are allowable in view of their dependency from the respective independent claims.

Conclusion

In view of the above, it is believed this application is in condition for allowance, and such a Notice is respectfully solicited.

To the extent necessary, Applicant petitions for an extension of time under 37 C.F.R. 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including any missing or insufficient fees under 37 C.F.R. 1.17(a) or 1.17(e), to Deposit Account No. 50-1130, under Order No. 95-456, and please credit any excess fees to such deposit account.

Respectfully submitted,

Leon R. Turkevich
Registration No. 34,035

Customer No. 23164
Date: January 4, 2007